CHAPTER 1

Overview

As the modern battlespace has become more sophisticated, military operations are executed in an increasingly complex electromagnetic environment. While military forces use the electromagnetic spectrum to detect and identify enemy forces and to perform communications, surveillance, and weapons systems operations, both military forces and civilians use the electromagnetic spectrum for communications, navigation, information gathering, processing, storing, and reporting. This overlapping usage of the electromagnetic spectrum complicates the military's use of its electronic equipment and the military's gathering and security of military information.

Successful military operations now greatly depend on control of the electromagnetic spectrum. The force that can deprive the enemy the use of the electromagnetic spectrum, exploit the enemy's use of the electromagnetic spectrum to obtain information for its own purposes, and control the electromagnetic spectrum will have an important advantage. During a conflict, all commanders attempt to dominate the electromagnetic spectrum by targeting, exploiting, disrupting, degrading, deceiving, damaging, or destroying their opponent's electronic systems that support their military operations. Electronic warfare (EW) includes "any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy." (Joint Publication [JP] 1-02) Electronic warfare is an important part of a military commander's arsenal of weapons. It allows a commander to provide electronic warfare support (ES), electronic attack (EA), and electronic protection (EP).

Electronic Warfare Support

Electronic warfare support (ES) is the "division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations." (JP 1-02) The ES intelligence collection effort—

- Is used in peace, crisis, and war, which contributes to the building of an EW/ intelligence database for planning and operations.

- Provides an all weather, day/night, long-range information gathering capability.
- Exploits an enemy's electromagnetic emissions and may provide information on enemy capabilities and intentions.
- Is covert and passive.
- Is a nonintrusive method of intelligence collection.

Electronic warfare support systems provide immediate threat recognition and are a source of information for immediate decisions involving electronic attack, electronic protection, avoidance, targeting, and other tactical employments of forces. Electronic warfare support systems collect data and produce information or intelligence that can be used to—

- Corroborate other sources of information or intelligence.
- Direct EA operations.
- Initiate self-protection measures.
- Task weapon systems for physical destruction.
- Support EP efforts.
- Create or modify EW databases.
- Support information operations (IO) activities.

Electronic warfare support data can be used to produce signals intelligence (SIGINT), provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. Electronic warfare support and SIGINT both involve searching for, intercepting, identifying, and locating sources of intentional or unintentional radiated electromagnetic energy. The primary differences between the two are the detected information's intended use, the degree of analytical effort expended, the detail of information provided, and the timelines required. Electronic warfare support is conducted for immediate threat recognition and provides information required for immediate tactical decisions. Signals intelligence is used to gain information concerning the enemy, usually in response to an intelligence requirement. See MCWP 2-15.2, *Signals Intelligence*, for more information.

ELECTRONIC ATTACK

Electronic attack (EA) is "that division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires." (JP 1-02)

Some common types of EA are spot, barrage, and sweep electromagnetic jamming. Electronic attack also includes various electromagnetic deception techniques such as false target or duplicate target generation.

Directed energy is "an umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles." (JP 1-02) A directed-energy weapon is a system that uses "directed energy primarily as a direct means to damage or destroy an enemy's equipment, facilities, and personnel." (JP 1-02)

Antiradiation weapons are weapons that use radiated energy emitted from the target as their mechanism for guiding onto a targeted emitter (e.g., high speed antiradiation missile system [HARM]).

ELECTRONIC PROTECTION

Electronic protection (EP) is "that division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability." (JP 1-02) In combat, electronic protection includes, but is not limited to, the application of good training and sound procedures for countering enemy electronic attack. United States forces (operators, users, and planners) must understand the enemy threat and the vulnerability of our electronic equipment to enemy EA efforts and ensure that appropriate actions are taken to safeguard our equipment from attack. To protect US forces, electronic protection must minimize an enemy's opportunity for successful ES and EA operations against US forces; therefore, it is necessary to—

- Regularly brief the EW threat to force personnel.
- Provide training on appropriate EP responses.
- Ensure that electronic system capabilities are safeguarded during exercises, workups, and pre-crisis training.

The technical aspects of EP must be considered when equipment acquisition programs are initiated. Equipment should be designed to limit inherent vulnerabilities. Additionally, these programs must be reviewed when EA vulnerabilities are detected.

Electronic protection measures include the selection of a scheme of maneuver that will minimize friendly electronic emissions that the enemy can intercept or disrupt using his ES and EA capabilities. Electronic protection can be accomplished through numerous methods; for example, a simple scheme of

maneuver that can be executed with few or no emissions, by imposing radio silence or emission control (EMCON) procedures, by selecting avenues of approach that interposes terrain between friendly transmitters and enemy intercept stations. Electronic protection also includes measures to minimize the vulnerability of friendly receivers to enemy jamming; for example, reduced power, brevity of transmissions, and directional antennas.

SPECTRUM MANAGEMENT

Spectrum management plays a key role in the successful planning and execution of electronic warfare. Spectrum management includes "planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference." (JP 1-02) Electronic warfare staff personnel have a major role to perform in the dynamic management of the electromagnetic spectrum during operations. Electronic warfare management activities are coordinated and deconflicted through the electronic warfare coordination cell (EWCC). The EWCC's primary mechanism for spectrum management is the restricted frequency list (RFL), which identifies friendly and enemy frequencies that cannot be jammed for various reasons. For further guidance on electromagnetic spectrum use, see Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3320.01, *Electromagnetic Spectrum Use in Joint Military Operations*. For specific guidance on reporting and controlling electromagnetic interference, see CJCSI 3320.02A, *Joint Spectrum Interference Resolution (JSIR)*.

AN/MLQ-36 Mobile Electronic Warfare Support System. The AN/MLQ-36 MEWSS provides a multifunctional capability that gives SIGINT/EW operators limited armor protection. This equipment can provide SIGINT/EW support to highly mobile mechanized and military operations in urban terrain where maneuver and/or armor protection is critical. MEWSS consists of a signals intercept system, a radio direction finding system, an EA system, a secure communications system, and an intercom system installed in a logistic variant of the light armored vehicle.

AN/MLQ-36A Mobile Electronic Warfare Support System Product Improvement Program. The AN/MLQ-36A MEWSS PIP is an advanced SIGINT/EW system integrated into a light armored vehicle. The MEWSS PIP provides a total replacement of the EW mission equipment now fielded in the AN/MLQ-36 MEWSS. The MEWSS PIP provides the ability to detect and evaluate enemy communications emissions, detect and categorize enemy noncommunications emissions (e.g., battlefield radars), determine lines of bearing, and degrade enemy tactical radio communications during expeditionary operations. When mission-configured and working cooperatively with other MEWSS PIP platforms, the common suite of equipment can also provide precision location of battlefield emitters. The system is designed to have an automated tasking and reporting data link to other MAGTF assets such as the AN/TSQ-130 technical control and analysis center PIP. The MEWSS PIP and its future enhancements will provide the capability to exploit new and sophisticated enemy electronic emissions and conduct electronic attack in support of existing and planned national, theater, fleet, and MAGTF SIGINT/EW operations.

MARINE TACTICAL ELECTRONIC WARFARE SQUADRON

The Marine VMAQ's mission is to provide EW support to the MAGTF and other designated forces. The VMAQ conducts tactical jamming to prevent, delay, or disrupt the enemy's ability to use early warning, acquisition, fire or missile control, counterbattery, and battlefield surveillance radars. Tactical jamming also denies and/or degrades enemy communications capabilities. The VMAQ conducts electronic surveillance operations to maintain electronic orders of battle, including both selected emitter parameters and location of nonfriendly emitters. It also provides threat warnings for friendly aircraft, ships, and ground units. VMAQ tasks include—

- Providing airborne EA and ES support to the ACE and other designated operations by intercepting, recording, and jamming threat communications and noncommunications emitters.

- Processing, analyzing, and producing routine and time-sensitive electronic intelligence (ELINT) reports for updating and maintaining enemy electronic order of battle. This is accomplished through the EW division, which includes intelligence, TERPES, and the tactical EA-6B mission planning system (TEAMS). All are used to support pre-mission planning and post-mission processing of collected data and production of pertinent intelligence reports. Working in concert with squadron intelligence, TERPES and TEAMS provide required ELINT and electronic order of battle intelligence products to the ACE, MAGTF, and other requesting external agencies.
- Providing liaison personnel to higher staffs to assist in VMAQ employment planning.
- Providing an air EW liaison officer to the MAGTF EWCC.
- Conducting EA operations for EP training of MAGTF units.

Organization

There are four VMAQs (designated VMAQ-1 through VMAQ-4) assigned to Marine aircraft group-14, 2d Marine aircraft wing, Cherry Point, NC. Each squadron has five EA-6B Prowler aircraft. Each squadron is organized into administrative, intelligence/EW, operations, logistic, safety and standardization, and maintenance divisions.

VMAQ Electronic Attack Equipment

EA-6B Prowler. The EA-6B Prowler is a subsonic, all-weather, carrier-capable aircraft. The crew is composed of one pilot and three electronic countermeasure officers. The EA-6B's primary missions include collecting and processing designated threat signals of interest for jamming and subsequent processing, analysis, and intelligence reporting and employing the AGM-88 HARM against designated targets. The EA-6B's AN/ALQ-99 tactical jamming system effectively incorporates receivers for the reception of emitted signals and external jamming pods for the transmission of energy to jam victim radars (principally those associated with enemy air defense radars and associated command and control). In addition to the AN/ALQ-99, the EA-6B also employs the USQ-113 communications jammer to collect, record, and disrupt threat communications.

Tactical EA-6B Mission Planning System. TEAMS assists the EA-6B aircrew with planning and optimization of receivers, jammers, and HARM. TEAMS allows an operator to—

- Maintain area of operations emitter listings.
- Edit emitter parameters.

- Develop mission-specific geographic data and electronic order of battle to—
  - Tailor or create HARM direct attack libraries or manually modify entries/ new threat cards for FA-18 HARM shooters.
  - Plan USQ-113 target selection.
- Perform post-flight mission analysis to—
  - Identify electronic emitters using various electronic parameter databases and ELINT analytical techniques.
  - Localize emitters by coordinates with a certain circular error of probability for each site.
  - Correlate new information with existing data.
  - Gather post-flight HARM information such as aircraft launch parameters, predicted seeker footprint, and whether the on board system detected a targeted signal at the time of impact.

Tactical Electronic Reconnaissance Processing and Evaluation System. The TERPES (AN/TSQ-90) is an air- and land-transportable, single-shelter ELINT processing and correlation system, and each of the four VMAQ squadrons includes a TERPES section. A TERPES section is composed of Marines, equipment, and software that identify and locate enemy radar emitters from data collected by EA-6B aircraft and those received from other intelligence sources, process and disseminate EW data rapidly to MAGTF and other intelligence centers, and provide mission planning and briefing support. TERPES support areas include operational support, intelligence analysis support, data fusion, fusion processing, intelligence reporting.

TERPES operational support—

- Translates machine-readable, airborne-collected digital data into man- and machine-readable reports (e.g., paper, magnetic tape, secure voice, plots, overlays).
- Receives and processes EA-6B mission tapes.
- Accepts, correlates, and identifies electronic emitter data from semiautomatic or automatic collection systems using various electronic parameter databases and various analysis techniques.
- Provides tactical jamming analysis.

The TERPES intelligence analysis application enables the operator to analyze ELINT data combined with additional modernized integrated database intelligence data to—

- Respond to intelligence requirements.
- Prepare intelligence database updates.
- Analyze threat and tactical situations.
- Estimate changes in the threat's tactical situation.

The modernized integrated database is the primary intelligence database for intelligence analysis application operator queries and provides data fusion capabilities. In addition to EA-6B aircraft mission tapes, the following inputs may also be fused to maximize the support provided to tactical intelligence operations:

- Naval intelligence database, which contains characteristics and performance data for weapons, sensors, and platforms.
- Electronic warfare database support, which is similar to the naval intelligence database and provides EA-6B tailored data.
- ELINT parameters list, which is the NSA's observed radar parametric data.
- Electronic warfare integrated reprogramming, which combines assessed technical radar parameters from the US Air Force EW Science and Technology database with the observed parameters of the NSA database.
- JSC, which is used to derive friendly electronic order of battle and radar parametric data.

Fusion processing is enabled by the TERPES fusion processor (TFP) and the TERPES ELINT preprocessor. The TFP processes intelligence data from tactical ELINT reports, sensor reports, tactical reports, and imagery intelligence reports. The TFP provides filtering, characteristic and performance identification, order of battle identification, technical analysis, multisource correlation, and candidate updates; and it presents the information in various forms for analysis. One TFP-integrated information source is the Tactical Related Applications Processor Data Dissemination System broadcast. This broadcast is accessed using the commander's tactical terminal and provides near real time, national-level reports to the TERPES. This broadcast also assists the TFP in maintaining an ELINT parameter database to track airborne, shipboard, and land-based targets. This data can be used to develop electronic orders of battle and to perform comparative studies on radar parameters.The TERPES ELINT preprocessor processes all EA-6B signals of interest collected from recorder or reproducer set tape or disk

files. Specifically, the application allows for the near real time analysis of technical ELINT data. Position reports and specific unit identification and location information are used to update the TERPES database and to prepare tactical ELINT reports. TERPES also provides tactical jamming system analysis for the EA-6B aircrew and maintenance personnel. Tactical jamming system analysis consists of recovering recorded data for verifying jammed calibration, jammer on and off times, and frequency and azimuth coverage. TERPES will use mission data in the generation of EW mission summary reports.

After-fusion processing intelligence reports are generated and the primary intelligence reporting output from TERPES is in the form of post-mission reports. Post-mission reports are provided in response to established intelligence requirements. See United States Signal Intelligence Directive (USSID) 340, *Tactical ELINT Reporting*, for the most commonly used reporting formats. Other report forms may include the following reports:

- Tactical reports provide information on immediate threat activity.
- ELINT summary reports provide a summary of ELINT activity over established periods (normally 24 hours). See USSID 200, *Technical SIGINT Reporting*, for format and content.
- ELINT technical reports provide for analyst exchange of information of parametric data. See USSID 341, *Technical ELINT Reporting*, for format and content.
- Over the horizon (OTH) “GOLD” reports provide information derived from contact reports of ELINT parametrics.
- Order of battle reports provide order of battle information such as basic encyclopedia number, equipment, and location.